

CLAIMS

WHAT IS CLAIMED IS:

1. A method for protecting a host located within a computer network, the
method comprising:

5 mapping a public host address for a public host to a secret host address for a
secret host containing data accessible over the computer network, said public host
address being available from a domain name system server;

receiving a request for communication with the secret host at the public host;
forwarding said request from the public host to the secret host; and
10 processing said request at the secret host and communicating from the secret
host over the network, wherein said communication appears to be sent from the
public host.

2. The method of claim 1 wherein the network is the Internet and the secret

15 host is a server.

3. The method of claim 2 wherein the server hosts a Web site.

4. The method of claim 1 wherein receiving a request comprises receiving a URL at the domain name system server, the domain name system server providing an IP address of the public host corresponding to the URL.

5. The method of claim 1 wherein forwarding said request comprises slowing down the forwarding of requests when the public host identifies an attack.

6. The method of claim 1 further comprising stopping the forwarding of said request when the public host identifies an attack.

7. The method of claim 6 further comprising notifying the secret host of the attack.

8. The method of claim 7 further comprising tracking down a source of the attack.

9. The method of claim 8 wherein tracking down a source of the attack comprises performing a trace back at the secret host.

5 10. The method of claim 1 further comprising directing one or more clients

to send requests to an alternate public host.

11. The method of claim 10 wherein a notification that the public host is under attack is received at the secret host.

10 12. The method of claim 10 wherein a notification that the public host is congested is received at the secret host.

13. The method of claim 10 wherein the secret host has received a request for heightened security.

15

14. The method of claim 10 further comprising requesting the DNS server to replace the public host address with an alternate public host address.

15. A computer program product for protecting a host located within a computer network, comprising:

computer code that maps a public host address for a public host to a secret host address for a secret host containing data accessible over the computer network,
5 said public host address being available from a domain name system server;

computer code that receives a request for communication with the secret host at the public host;

computer code that forwards said request from the public host to the secret host;

10 computer code that processes said request at the secret host and communicates from the secret host over the network, wherein said communication appears to be sent from the public host; and

a computer-readable storage medium for storing the codes.

15 16. The computer program product of claim 15 wherein the computer readable medium is selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, hard drive, and data signal embodied in a carrier wave.

17. The computer program product of claim 15 further comprising code that receives at the secret host a notification that the public host is under attack.

5 18. The computer program product of claim 17 further comprising code that directs one or more clients to send requests to an alternate public host upon receiving said notification.

10 19. The computer program product of claim 17 further comprising code that requests the DNS server to replace the public host address with an alternate public host address upon receiving said notification.

15

20. A system for protecting a host located within a computer network, the
system comprising:

a public host having a public host address available from a DNS server; and
a secret host having a secret host address and containing data accessible over
the computer network, said public host address being mapped to said secret host
address;

wherein the public host is operable to forward requests received from the
network to the secret host and the secret host is operable to process said requests and
communicate from the secret host to the network with said communication appearing
to be sent from the public host.

10
15
21. The system of claim 20 wherein the secret host is configured to manage
the public host.

22. A method for hiding an IP address of a computer node located within a computer network, the method comprising:

associating an IP address for a public node with an IP address of a secret node such that only the public node has access to the IP address of the secret node,

5 said IP address for the public node being available from a DNS server;

receiving packets from the network at the public node;

forwarding said packets from the public node to the secret node; and

responding to said packets at the secret node such that a response appears to be sent from the public node rather than the secret node.

10
23. The method of claim 22 wherein the packets contain requests for data and the secret node is a server hosting a Web site.

24. The method of claim 22 wherein the packets contain e-mail.

15
25. The method of claim 22 further comprising stopping the forwarding of packets when the public node is under attack.

5

26. The method of claim 25 further comprising requesting the DNS server to replace the IP address of the public node with an IP address of an alternate public node.

27. The method of claim 25 further comprising directing specific client

computers to send packets directed at the public node to an alternate public node.

28. The method of claim 22 further comprising switching to an alternate public host when congestion at the public host exceeds a predetermined level.

10

29. The method of claim 22 further comprising switching to an alternate public host to provide increased security at the secret host.